PowerFolder Open Cloud Mesh (v0.0.3) Integration

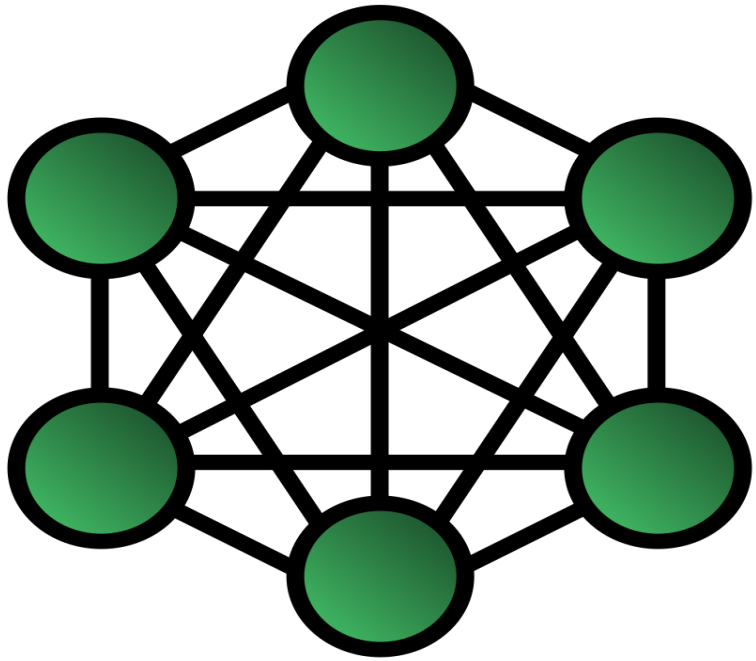
Jan Wiegmann

Table Of Contents

1. Introduction
2. OCM API Endpoints
3. Trusted Relationships
4. Discovery Service

What Is A Federated Network?

- Network of clouds
- All clouds trust each other
- OCM: Interface for interactions between clouds



OCM Integration Into PowerFolder

- Successful use of federated networks for more than one year
- Use cases:
  1. Federated sharing
  2. Federated login
  3. Federated notifications

- OCM integration since PowerFolder Server 11.5

OCM API Endpoints

1. Retrieve a single share:

   GET ⟶ /shares/id

2. Retrieve all shares:

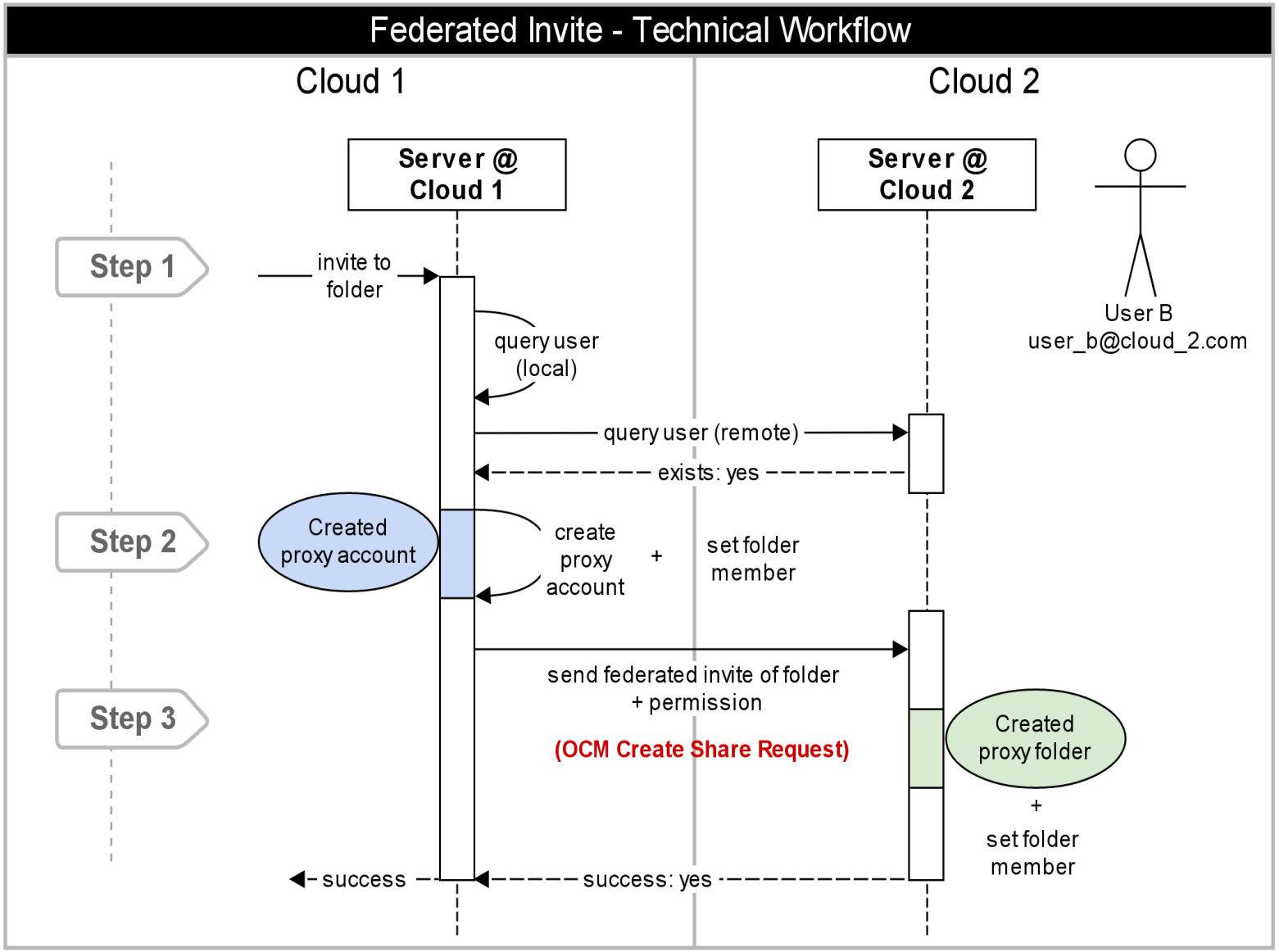
   GET ⟶ /shares

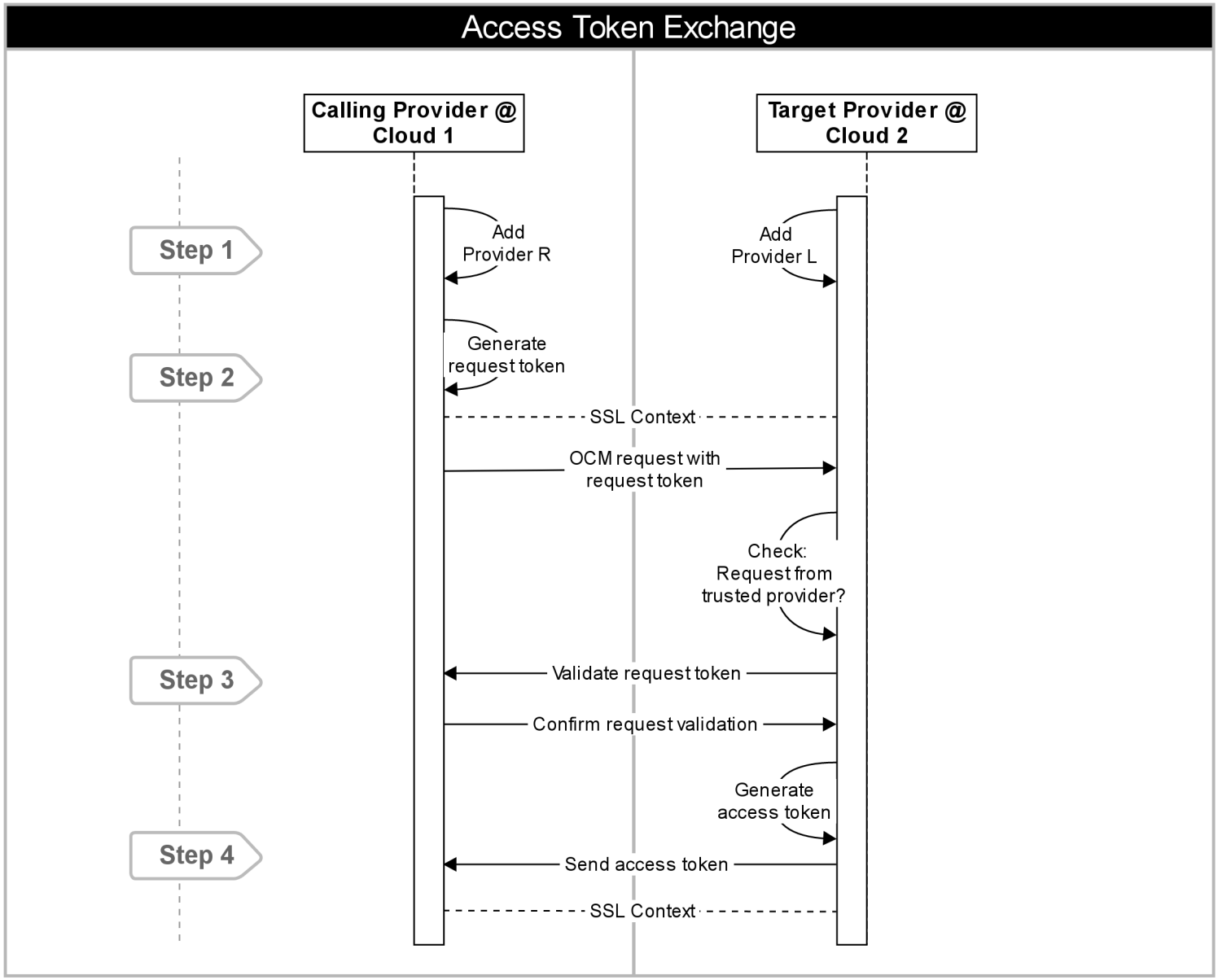
3. Create a share (Invite):

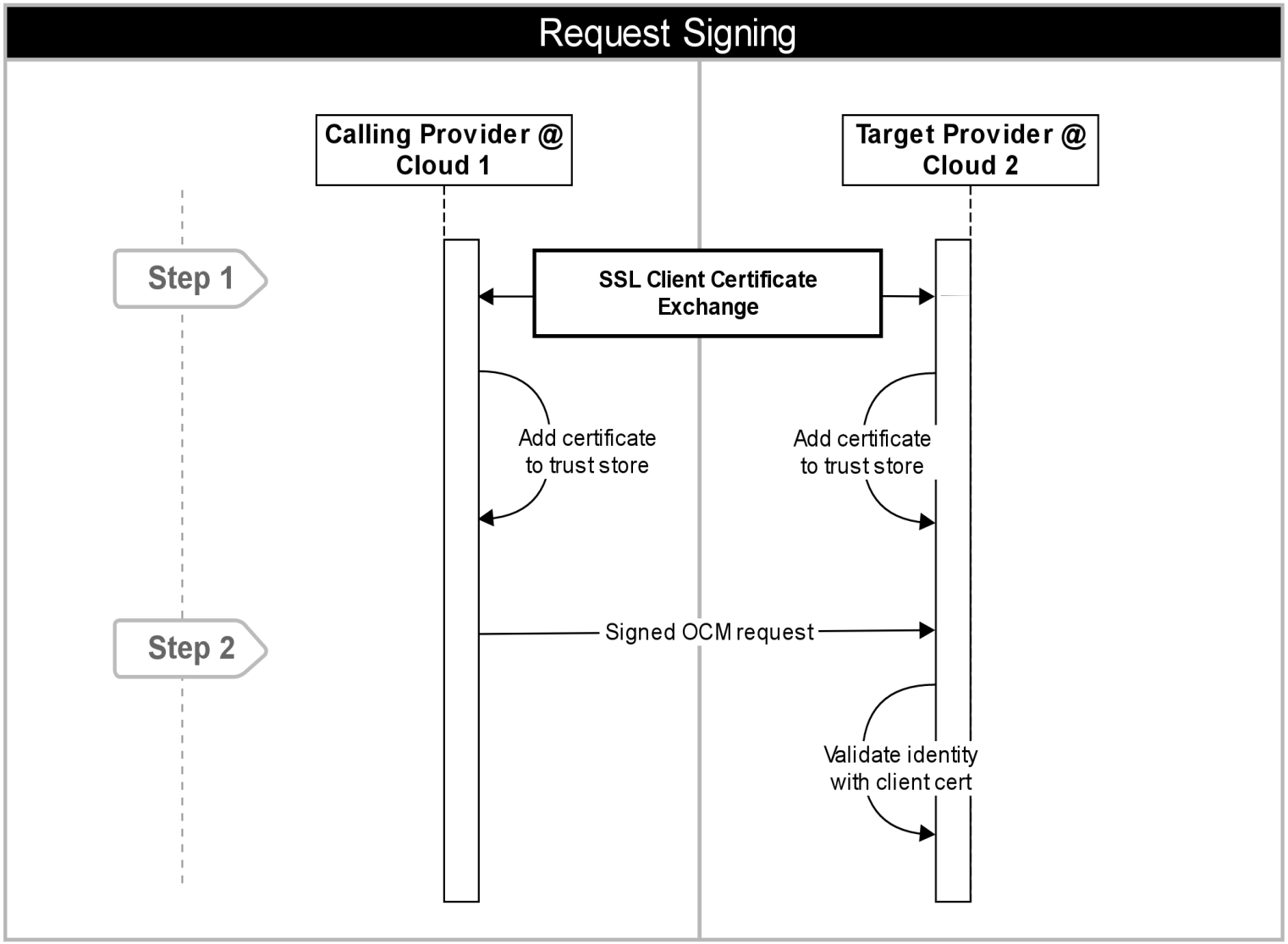
   POST ⟶ /shares

Create Share Request Body

```
{
    "shareId": "5a251569506eb81f477a67dd",
    "owner": "user@cloud1.de",
    "shareWith": "user@cloud2.de",
    "permission": "read_write",
    "name": "foo",
    " description ": "foobar",
    " providerId ": "cec0c932ce01",
    "protocol": [
        {"name": "pf_classic",
            "options": { "access_token" : "foobar9000" }
        },
        ...
    ]
}
```


Federated Invite - Technical Workflow
Cloud 1
Cloud 2
Server @ Cloud 1
Server @ Cloud 2
User B
user_b@cloud_2.com
Step 1
invite to folder
query user (local)
query user (remote)
exists: yes
Step 2
Created proxy account
create proxy account
+
set folder member
send federated invite of folder + permission
(OCM Create Share Request)
Step 3
Created proxy folder
+
set folder member
success
success: yes


Access Token Exchange
Calling Provider @ Cloud 1
Target Provider @ Cloud 2
Step 1
Add Provider R
Add Provider L
Step 2
Generate request token
SSL Context
OCM request with request token
Check: Request from trusted provider?
Step 3
Validate request token
Confirm request validation
Generate access token
Step 4
Send access token
SSL Context

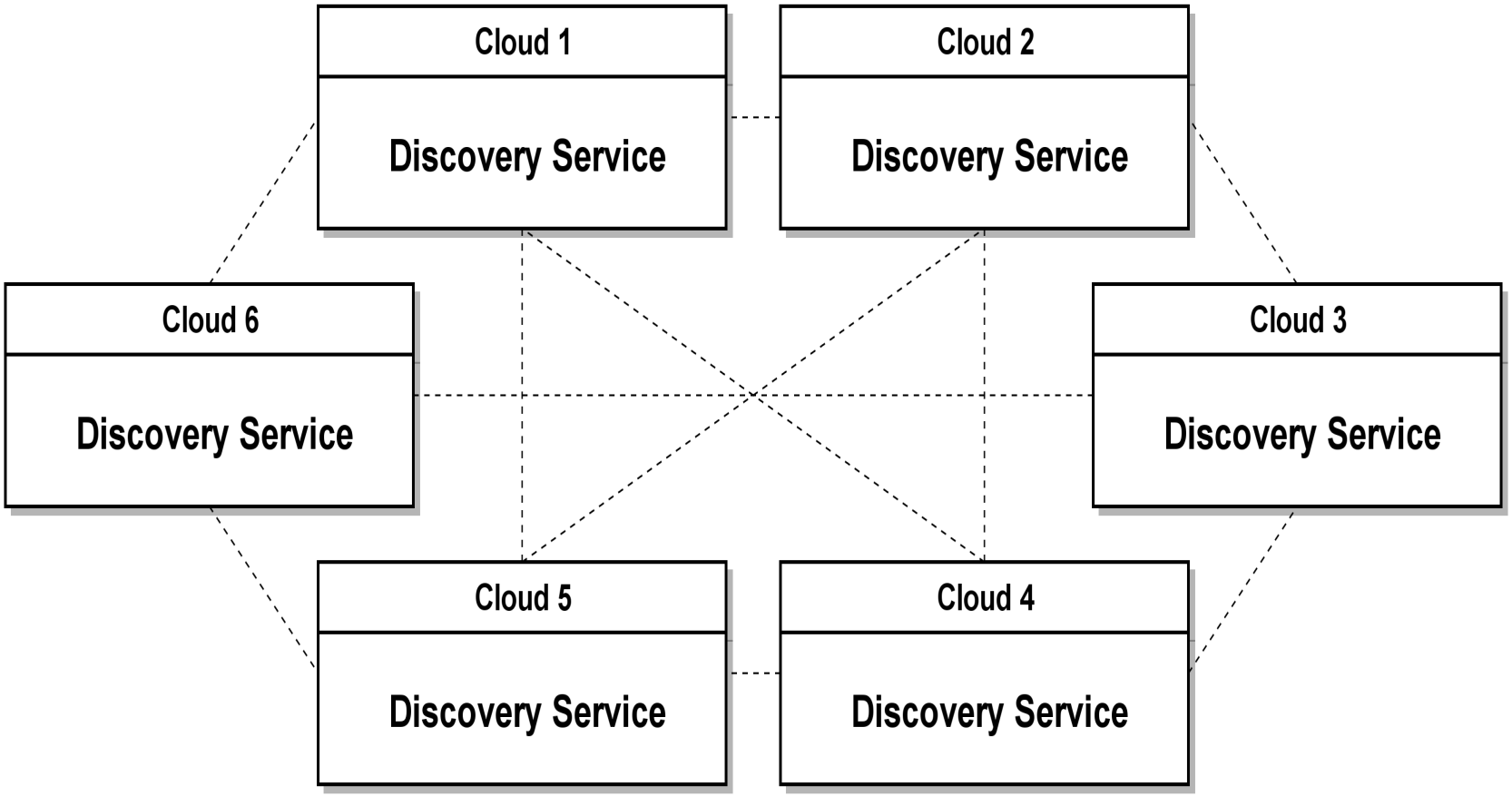

Request Signing
Calling Provider @ Cloud 1
Target Provider @ Cloud 2
Step 1
SSL Client Certificate Exchange
Add certificate to trust store
Add certificate to trust store
Step 2
Signed OCM request
Validate identity with client cert

Conclusion

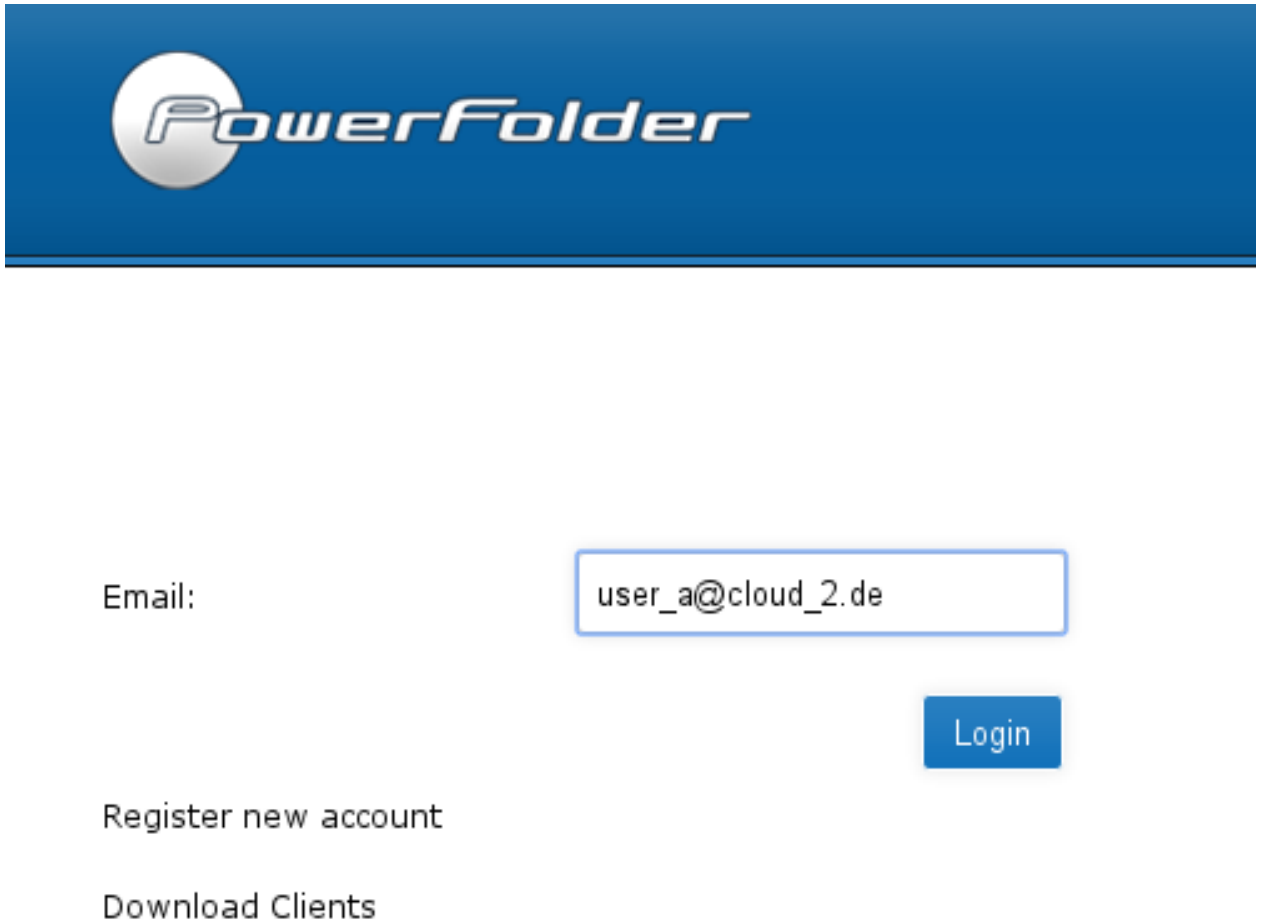
+ Easy administration:
  - Usage in large networks with trust providers

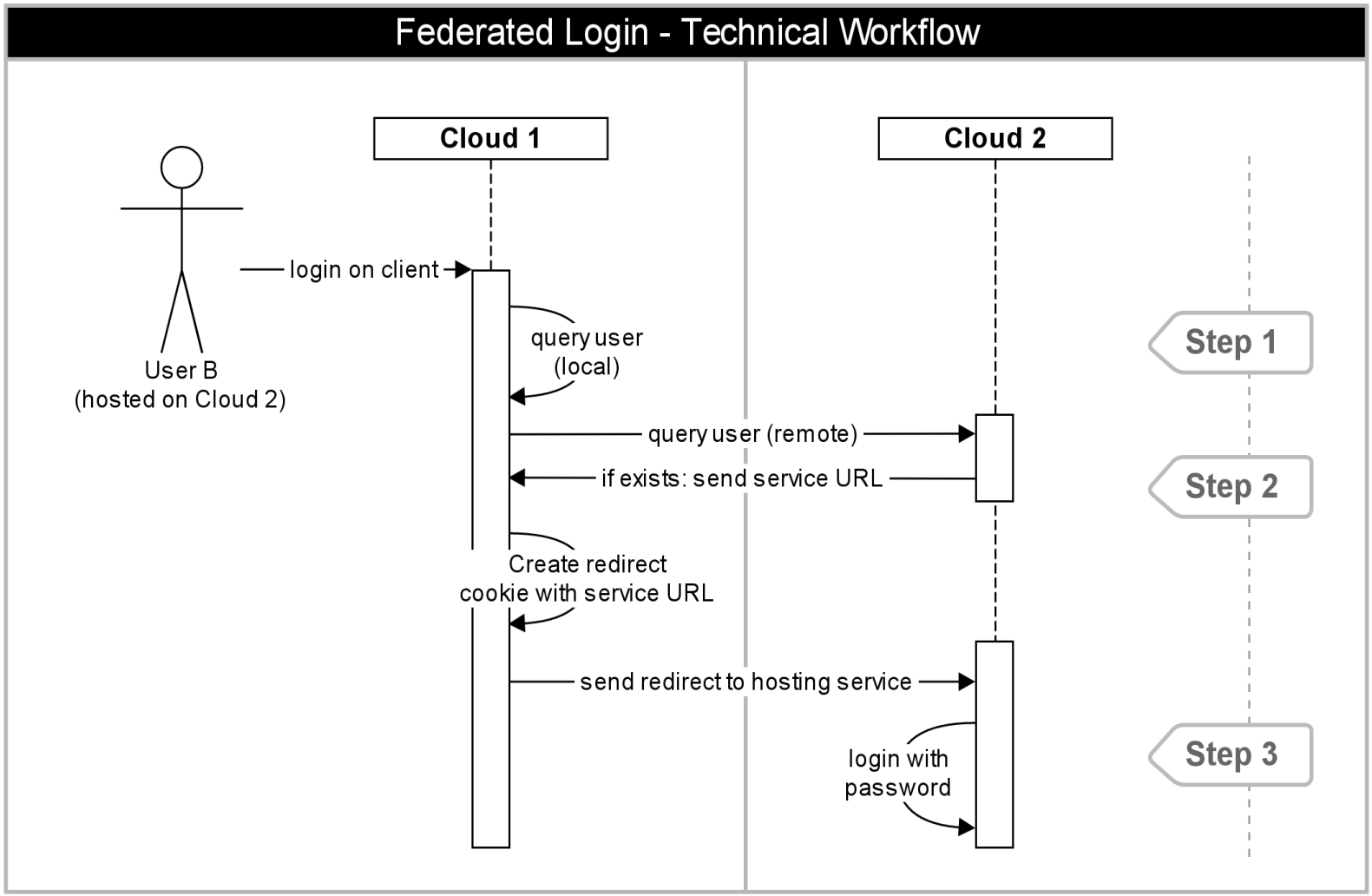
+ Strong security:
  - Request validation by SSL client certificate authentication

Discovery Service



Federated Web-Login @ Cloud 1




Federated Login - Technical Workflow
Cloud 1
Cloud 2
User B
(hosted on Cloud 2)
login on client
query user
(local)
query user (remote)
if exists: send service URL
Create redirect
cookie with service URL
send redirect to hosting service
login with
password
Step 1
Step 2
Step 3

Thank you!

Jan Wiegmann
wiegmann@powerfolder.com
www.powerfolder.com